UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,214	01/29/2002	Robert J. Lambert	00001-0423	2205

7590 03/24/2005

Orange & Chari
66 Wellington Street West
Toronto Dominion Bank Tower
Toronto, ON M5K 1H6
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,214	LAMBERT ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/08/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on January 29, 2002. Claims 1-12 were originally received for consideration. No preliminary amendments for the claims were filed. Claim 1-12 is currently under consideration.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 8 recites the limitations "m," in the equation providing the quotient. There is insufficient antecedent basis for this limitation in the claim and the claim becomes indefinite as there are no defined bounds for the variable "m."

3. Claim 10 recites the limitation "said endomorphism" in the final limitation of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. The claimed invention is directed to non-statutory subject matter. Claims 1-12 fail to transform a physical subject matter to a different state, as the steps recited in the

claim represent a computation of a point multiple in conjunction with data gathering, or making available other data, as required by the computation. As such, no specific physical manipulation of the math algorithm is realized in the claim when the algorithm is instantiated. Therefore, the claim 1 is non-statutory under the abstract idea exception. See MPEP IV.B.1.

5. The claimed invention is directed to non-statutory subject matter. Claim 1 further discloses a "data carrier." This "data carrier" is not defined in the claims nor the specification, and can be interpreted as a "signal" which recites nothing but the physical characteristics of a form of energy, which is non-statutory. See MPEP IV.B.1(c).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Kobayashi et al. (U.S. Patent No. 6,430,588).

Regarding claim 1, Kobayashi discloses:

A method of providing a point multiple in an elliptic curve cryptosystem, said point multiple being derived from a scalar and a point on an elliptic curve having an equation of the form y.sup.2+xy=x.sup.3+a.sub.1x.sup.2+1, where al is either 0 or 1, said method comprising the steps of:

a) obtaining a pair of coefficients derived from a truncator of said elliptic curve (column 3 lines 25-52, column 6 lines 8-46);

b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and a Frobenius mapping .tau.(column 1 line 63 – column 12 line 16, column 11 lines 40-49);

d) providing said point multiple to said elliptic curve cryptosystem (column 3 lines 25-52, column 12 lines 26-30).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Kobayashi discloses:

A method according to claim 1, wherein said pair of coefficients corresponds to an approximation of the inverse of said truncator (column 3 lines 25-52, column 6 lines 8-46).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Kobayashi discloses:

A method according to claim 2, wherein said approximation is determined by a significance parameter (column 3 lines 25-52, column 6 lines 8-46).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Kobayashi discloses:

A method according to claim 1, wherein said representation of said scalar is equivalent to said scalar modulo said truncator (column 3 lines 25-52, column 6 lines 8-46).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Kobayashi discloses:

A method according to claim 2, further comprising the step of computing a quotient derived from said pair of coefficients and said scalar and using said quotient to perform the step of computing said representation of said scalar (column 3 lines 25-52, column 11 line 46 – column 12 line 29).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Kobayashi discloses:

A method according to claim 5, wherein said quotient is equivalent to a product of said scalar and said approximation of said inverse of said truncator (column 3 lines 25-52, column 11 line 46 – column 12 line 29).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Kobayashi discloses:

A method according to claim 6, wherein said representation of said scalar is equivalent to a remainder after division of said scalar by said truncator (column 3 lines 25-52, column 11 line 46 – column 12 line 29).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Kobayashi discloses:

A method according to claim 1, wherein said truncator is (tau .sup(m) – 1) / (tau – 1) (column 3 lines 25-52, column 11 line 46 – column 12 line 29).

Regarding claim 9, Kobayashi discloses:

A method of computing a key derived from a scalar and a point on an elliptic curve having an equation of the form y.sup.2+xy=x.sup.3+a.sub.1x- .sup.2+1, where a, is either 0 or 1, said method comprising the steps of:

a) obtaining a pair of coefficients derived from a truncator of said elliptic curve (column 3 lines 25-52, column 6 lines 8-46);

b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and a Frobenius mapping .tau (column 1 line 63 – column 2 lines 11, column 11 lines 40-49).

Regarding claim 11, Kobayashi discloses:

In a method of computing an elliptic curve digital signature requiring a point multiple, the improvement comprising computing said point multiple by the steps of:

a) obtaining a pair of coefficients derived from a truncator of said elliptic curve (column 3 lines 25-52, column 6 lines 8-46);

b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve (column 3 lines 25-52, column 11 line 46 – column 12 line 29);

c) computing said point multiple using said representation of said scalar and said endomorphism of said elliptic curve (column 1 line 63 – column 2 line 16, column 11 lines 40-49).

7. Claim 11 is a data carrier containing computer executable instructions claim analogous to claim 1, and therefore, is rejected following the same reasoning.

8. Claim 12 is a system claim analogous to the method claim of claim 1, and therefore, is rejected following the same reasoning.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA KA.
03/21/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100